Some Mathematical Properties of a Scheme for Reducing the Bandwidth of Motion Pictures by Hadamard Smearing

By E. R. BERLEKAMP

(Manuscript recieved September 29, 1969)

M. R. Schroeder recently proposed a scheme for compression of motion picture data by taking the difference of two successive frames and then smearing.[1] *The smearing is accomplished by a Hadamard matrix.*

If the Hadamard matrix is of a certain particularly well-understood type, then we show that if the input differential picture consists of a small odd number of large pulses of identical magnitudes (but arbitrary signs), then the output will consist of three components:

(i) Large pulses of equal magnitude and the correct signs, matching each of the input pulses.

(ii) One additional "stray" large pulse, of magnitude equal to the others, but located at a point where the input was zero.

(iii) Scattered pulses of amplitude low relative to the pulses of types i and ii, but so numerous that they consume $(\pi - 2)/\pi$ *of the total energy of the output differential picture.*

We give an explicit formula for the amplitude of each of these pulses.

The problem of determining the distributions of all possible outputs of the proposed system for other classes of inputs is shown to be equivalent to the unsolved problem of finding the weight enumerators for the cosets of the first order Reed-Muller codes.

I. INTRODUCTION

The fact that successive frames of a motion picture are often very nearly alike has led to the consideration of schemes which transmit, for each point of the picture, the difference between the amplitude of the present frame and the amplitude of the previous frame. Since

this differential picture* is frequently zero at many points, there is reason to hope that the bandwidth required for transmission of the differential picture could be greatly reduced by appropriate coding.

One such coding scheme which has been considered by W. K. Pratt, J. Kane, and H. C. Andrews,[2] and refined by M. R. Schroeder[1] is the following: let the differential picture be represented by a real n-dimensional vector, $\mathbf{v}$. (For example, if the picture is represented by a 100×100 grid, then $n = 10000$.) Let $\mathcal{H}$ be an $n \times n$ *Hadamard* matrix, which is a self-orthogonal real matrix all of whose entries are ± 1, and let the smeared differential picture (or transformed differential picture), $\mathbf{x}$, be defined by $\mathbf{x} = \mathcal{H}\mathbf{v}/(n)^{\frac{1}{2}}$. Let Q be the power-preserving clipping operator, defined by

$$Q\mathbf{x} = \frac{(||\mathbf{x}||)^{\frac{1}{2}} \operatorname{sgn}(\mathbf{x})}{(n)^{\frac{1}{4}}},$$

where sgn $(\mathbf{x})$ is the n-dimensional vector whose ith component is $+1$ or -1, depending on the sign of the ith component of $\mathbf{x}$. Since we wish the quantizer to have only two outputs, we cannot take sgn $(0) = 0$. Unless stated otherwise, we assume that sgn (0) is undefined. Schroeder has asserted that the vector $\mathbf{y} = Q\mathbf{x} = Q\mathcal{H}\mathbf{v}/(n)^{\frac{1}{2}}$ provides an appropriate "encoding" of the differential picture $\mathbf{v}$. To "decode" one computes $\mathbf{z} = 1/(n)^{\frac{1}{2}}\mathcal{H}'\mathbf{y}$. The question to be studied in this paper is the quality of z as an approximation to $\mathbf{v}$.

Some of the heuristic arguments favoring this proposed scheme are the following: Since successive frames are frequently very similar, the differential picture will have near-zero amplitude at most points. In a typical case when the camera is focused on a moving subject and a fixed background, the differential picture will be identically zero at all background points. If the subject and the background each has uniform color (the simplest plausible case), then the differential picture will be nonzero only at those points on the boundary of the subject. Furthermore, all of the nonzero amplitudes in the differential picture will have equal magnitudes, although their signs will depend on whether they are on the leading or trailing edge of the moving subject. The

* To be precise, the "differential picture" *should* consist of the difference between what the present frame actually is and what the decoder thought the last frame was. Since all of the errors in the system are assumed to arise from quantization, rather than from any sort of unpredictable noise on the communications channel, the encoder may include a replica of the decoder, thereby enabling it to compute what the decoder thought the last frame was. Each transmitted differential picture then includes an attempt to correct the cumulative effects of all previous errors. In this paper, we study only the quantization noise introduced in the encoding and decoding of a single differential picture, ignoring the complicated dynamic questions which arise when one studies the behavior of the system during several successive frames.

conventional manner of encoding the differential picture is to quantize the amplitude at each gridpoint. This scheme will introduce no quantization error at all on the background points, which have zero amplitude, but a relatively high number of quantization levels may be required to keep the quantization errors along the outline of the subject down to a tolerable level. The Hadamard transform of the differential picture, on the other hand, will have its energy spread out relatively uniformly among the grid points. A coarse quantization of the smeared differential picture will introduce quantization errors throughout the differential picture in a relatively uniform manner. When the quantized smeared differential picture is unsmeared, the quantization errors, being somewhat independent, should tend to cancel out. It is thus hoped that a coarser quantization of the smeared differential picture might yield a decoded differential picture of the same fidelity as a substantially finer quantization of the original, unsmeared differential picture.

A somewhat more theoretical discussion of the effects of quantization in the Hadamard transform domain is given in Section VI of Pratt, Kane, and Andrews.[2] The main result is that the Hadamard transformation preserves energy. Hence, if the amplitudes at the various points in the transformed differential picture are independent zero mean gaussian random variables, then the energy of the noise introduced by a two-level quantizer would be $(\pi - 2)/\pi$ of the total energy in the output differential picture, both before and after unsmearing. From this viewpoint, the major attraction of smearing is that it distributes the quantization noise uniformly throughout the picture. If our simple model of a differential picture (which has nonzero amplitude only along the outline of the subject) is coarsely quantized, then all of the quantization noise appears on the outline, where it will tend to blur the subject. However, if this differential picture is smeared, coarsely quantized, and unsmeared, then its quantization noise should be evenly distributed throughout the subject and the background.

We shall now study the relationship between the original differential picture, $\mathbf{v}$, and the decoded differential picture, $\mathbf{z}$. It is clear that the energy in the vector $\mathbf{z}$ is always identical to the energy in the vector $\mathbf{v}$. Hence, for purposes of analysis, it is easiest to compute $\mathbf{z}$ according to the formula

$$\mathbf{z} = A\mathcal{H}^t \operatorname{sgn} \mathcal{H}\mathbf{v}$$

where for each frame A is a non-negative scalar chosen to make the energy in $\mathbf{z}$ equal to the energy in $\mathbf{v}$. In this paper, we often omit the actual calculation of A.

In the case where $\mathbf{v}$ has only one nonzero component, then sgn $\mathcal{H}\mathbf{v} = \mathcal{H}\mathbf{v}$ and $\mathbf{z} = A\mathcal{H}^t\mathcal{H}\mathbf{v}$. Since $\mathcal{H}^t\mathcal{H} = nI$ (where I is the $n \times n$ identity matrix) it follows that $\mathbf{z} = \mathbf{v}$. In other words, the system transmits a single pulse without error.

On the other hand, when $\mathbf{v}$ has only two nonzero components, then the component with the larger amplitude dominates the component with the smaller amplitude. In this case $\mathbf{z}$ again has a single nonzero component, even though $\mathbf{v}$ had two nonzero components. However, the choice $\mathbf{v} = [1, 1-\epsilon, 0, 0, 0, \cdots, 0]$ results in an ambiguity. If we instead write $\mathbf{v} = [1, 1, \epsilon, 0, 0, 0, \cdots, 0]$, then we may actually find that, in the limit as $\epsilon \to 0$, $\mathbf{z} \to [1, 1, 0, 0, \cdots, 0]$. If $\mathbf{v} = [1, 1, 0, 0, \cdots, 0]$, then $\mathbf{z}$ is undefined because it depends on sgn 0, which is either plus or minus. In fact, $\mathbf{z}$ is undefined whenever $\mathbf{v}$ has an even number of nonzero components, all of equal magnitude; but this difficulty might be removable by adding an appropriate background noise function into $\mathbf{v}$, or by choosing sgn(0)'s independently at random. To avoid the necessity of such considerations, we devote our primary attention in this paper to the case in which $\mathbf{v}$ has an *odd* number of nonzero components, all of unit magnitude (but arbitrary sign). In this case, every component of $\mathcal{H}\mathbf{v}$ is an odd integer. Since every component of $\mathcal{H}\mathbf{v}$ must therefore have magnitude at least 1, the sgn function is defined and the analysis remains valid in the presence of a small background noise in any or all components of $\mathbf{v}$.

II. HADAMARD MATRICES

The requirement that any three rows of a Hadamard matrix be pairwise orthogonal leads to the immediate conclusion that if $n > 2$, then an $n \times n$ Hadamard matrix can exist only if n is a multiple of 4. The question of whether or not there actually do exist $n \times n$ Hadamard matrices for all $n \equiv 0 \bmod 4$ is now one of the most intriguing unsolved problems in combinatorial theory. Many ingenious constructions have been proposed, and several of them succeed in obtaining Hadamard matrices for an infinite number of (scattered) values of n. For example, if n is a multiple of 4 and $n - 1$ is a prime-power, then a well-known construction based on quadratic residues in the finite field $GF(n-1)$ yields an $n \times n$ Hadamard matrix. Many other constructions for Hadamard matrices are given in Chapter 14 of Hall,[3] and more recent constructions have been presented by Spence,[4] Goethals and Seidel,[5] and Wallis.[6,7] The smallest value of $n \equiv 0 \bmod 4$ for which no $n \times n$ Hadamard matrix has yet been constructed is $n = 188$.

For many values of n, there exist Hadamard matrices with additional structure. For example, some Hadamard matrices have the property that the first row and first column consist entirely of +1's, and the remaining $(n-1) \times (n-1)$ submatrix has the property that each of its rows is a cyclic shift of the previous row. Such matrices are called *cyclic* Hadamard matrices. They are known to exist whenever $n-1$ is prime, or when $n-1$ is the product of twin primes, or when n is a power of 2. A computer search by Thoene & Golomb[8] and some calculations by Baumert[9] have shown that no cyclic Hadamard matrices of other orders less than 1000 exist, with the possible exceptions of $n = 400, 496, 628, 652, 784, 976$.

From the viewpoint of an algebraic coding theorist, a shortened Hadamard matrix (obtained from a standard Hadamard matrix by multiplying each row by an appropriate sign to make the first column all +1's, and then deleting the first column) is equivalent to an *equidistant binary code*. The n codewords are taken as the rows of the shortened Hadamard matrix, with each +1 replaced by 0 and each −1 replaced by 1. Since the dot product of any pair of rows in the shortened Hadamard matrix is −1, the distance between any pair of words in the binary code is $(n+1)/2$. Further discussion of such codes is given in Section 13.5 of Berlekamp.[10]

The best-understood class of equidistant binary codes is the maximal-length shift-register codes, which are also called shortened first-order Reed-Muller codes. In addition to being cyclic and equidistant, they are *linear* over the binary field, which means that the component by component binary sum of any pair of codewords is another codeword. Stated in terms of the original Hadamard matrices, this property means that the componentwise product of any pair of rows of the Hadamard matrix is another row of the same Hadamard matrix. Although Hadamard matrices with this property are relatively rare, they exist for every n which is a power of 2. Because of their correspondence to the Reed-Muller codes, these matrices are comparatively well-understood, and we shall henceforth confine our discussion to Hadamard matrices of this type. Such matrices may be taken as cyclic.

III. THE INDUCED COORDINATIZATION

A $2^k \times 2^k$ Hadamard matrix corresponding to a Reed-Muller code induces a (non-unique) coordinatization on the 2^k components of each row, associating each component with a k-dimensional vector over $GF(2)$. A set of 2^i coordinates is said to form an affine subspace iff the

corresponding 2^j k-dimensional vectors form an affine j-dimensional subspace over $GF(2)$. Similarly, a set of m coordinates are said to be linearly (or affine) independent iff the corresponding k-dimensional vectors are linearly (or affine) independent.

If a set of m binary k-tuples α_1 , α_2 , $\cdots$ α_m are affine independent, then they span an $(m - 1)$-dimensional affine subspace, each element of which has a unique representation of the form

$$\sum_{i=1}^{2^j+1} \alpha_{i_1}$$

for some j. A set of binary vectors are affine independent iff no subset containing an even number of vectors sums to zero. An affine basis for the set of all 2^k binary k-dimensional vectors may be selected in various ways. The "standard" basis consists of the all-zero vector and each of the k "unit" vectors. In general, any $k + 1$ affine independent vectors may be chosen as a basis.

If k is very large, then the probability that a randomly chosen set of $k + 1$ k-dimensional binary vectors will be affine independent is $\prod_{i=1}^{\infty} (1 - 2^{-i})$, or about 29 percent. The probability that k randomly chosen vectors will be affine independent is about 58 percent; for $k - 1$, it is 76 percent. If $m \ll k$, then almost every set of m different k-dimensional binary vectors is affine independent.

The first row of the $2^k \times 2^k$ Hadamard matrix may be taken as all $+1$'s. The 2^{k-1} $+1$'s in each of the other rows occur in the components corresponding to some $(k - 1)$-dimensional subspace of the k-dimensional binary vectors, and the -1's occur in the components corresponding to the complementary $(k - 1)$-dimensional affine subspace.

The coordinatization induced by the Hadamard matrix is invariant under all changes of affine basis. When translated into coding terminology, this is equivalent to Theorem 15.35 of Berlekamp.[10]

IV. MAIN RESULT AND DISCUSSION

4.1 *Theorem*

Let $\mathbf{v}$ be a 2^k-dimensional vector whose only nonzero components are $2m + 1$ units occurring at components corresponding to k-dimensional binary vectors α_0 , α_1 , α_2 , $\cdots$ α_{2m} which are affine independent. Let the vector $\mathbf{z}$ be defined by the equation

$$\mathbf{z} = \mathcal{H}^t \operatorname{sgn} \mathcal{H}\mathbf{v}.$$

Then the value of z_β , the component of $\mathbf{z}$ corresponding to the k-

dimensional binary vector β, is given by

$$z_\beta = \begin{cases} 0 & \text{if } \beta \text{ is not in the affine subspace spanned by} \\ & \alpha_0 , \alpha_1 , \alpha_2 , \cdots , \alpha_{2m} \\ \dfrac{S 2^{k-2m}(2m - 2j)!\,(2j)!}{j!\,m!\,(m - j)!} & \text{if } \beta = \sum_{l=1}^{2j+1} \alpha_{i_l} \end{cases}$$

and the sign is given by

$$S = (-1)^j \prod_{l=1}^{2j+1} v_{\alpha_{i_l}}.$$

4.2 *Remarks*

We first notice that the answers do not significantly depend on k, but on $2m + 1$, the number of units in the input vector **v**.

Since **z** is defined by an equation of the form $\mathbf{z} = 3\mathfrak{C}'\mathbf{y}$, where the energy of **y** is n, the energy of **z** is $n^2 = 4^k$. For $i = 0, 1, \cdots 2m$ we have

$$| z_{\alpha_i} |^2 = \left[2^{k-2m} \binom{2m}{m} \right]^2.$$

For large m, $| z_{\alpha_i} |^2$ is closely approximated by $2^{2k}/\pi m$. Thus only $2/\pi$ of the total energy in **z** is located in those components in which **v** has units; the remaining $(\pi - 2)/\pi$ of the total energy is distributed throughout the affine subspace. For example, if $m = 5$, $k = 10$, we have the following output:

Input Value	Corresponding Output Value	$\binom{\text{Output}}{\text{Value}}^2$	Number of such Coordinates
1	252	16×3969	$\binom{11}{1} = 11$
0	28	16×49	$\binom{11}{3} + \binom{11}{9} = 220$
0	12	16×9	$\binom{11}{5} + \binom{11}{7} = 792$
0	252	16×3969	$\binom{11}{11} = 1$
Totals		16×2^{16}	1024

For all m, we notice that if $\beta = \sum_{i=0}^{2m} \alpha_i$, then

$$| z_\beta | = | z_{\alpha_i} |.$$

In other words, if the input to the coding-transmission-decoding system consists of $2m + 1$ pulses of equal magnitudes (and arbitrary signs)

located at positions which are affine independent then the output may he written as the sum of the following three terms:

(*i*) $2m + 1$ pulses of equal magnitude (and correct signs) matching the input.
(*ii*) One stray pulse of the same magnitude as the $2m + 1$ correct ones.
(*iii*) Other errors scattered throughout the affine subspace, having maximum amplitude $[1/(2m - 1)]$ times as large as the correct pulses.

Since each of the errors of type *iii* has a relative amplitude approaching zero for sufficiently large m, one might consider the proposed system "successful" in some sufficiently broad sense of that term even though these errors consume $(\pi - 2)/\pi$ of the energy in the output signal. The error of type *ii* poses a different problem, even though it consumes a negligible fraction of the energy. Further research may be required to decide whether these difficulties might be removed by replacing the operator Q by another quantizer with more levels. Further study will also he required to determine how these quantization errors propagate in successive frames in a dynamic system. (See footnote on page 970.)

V. RELATIONSHIP TO THE WEIGHT ENUMERATION PROBLEM FOR RM COSETS

In the previous sections we calculated the vector $\mathbf{z} = \mathcal{H}'Q\mathcal{H}\mathbf{v}$ for certain specific choices of $\mathbf{v}$. These vectors $\mathbf{v}$ were chosen to be "typical" in some intuitive sense, and yet sufficiently simple in form to enahle us to carry through the calculation in closed form, even when the dimensions of the $\mathcal{H}$ matrix $(n \times n)$ were large.

Instead of assuming some ad hoc form for the vector $\mathbf{v}$, we might instead ask, what is the range of the operator $\mathcal{H}'Q\mathcal{H}$? Except for the scalar factor, this is equivalent to determining thc range of the operator $\mathcal{H}'$ sgn. For, if there exists a vector $\mathbf{x}$ such that $\mathbf{z} = \mathcal{H}'$ sgn $\mathbf{x}$, then n sgn $\mathbf{x}$ = sgn $\mathcal{H}\mathbf{z}$ and $\mathbf{z} = (\mathcal{H}'$ sgn $\mathcal{H}\mathbf{z})/n$. Hence, every vector in the range of $\mathcal{H}'$ sgn is proportional to a vector in the range of $\mathcal{H}'Q\mathcal{H}$, and every vector in the range of $\mathcal{H}'Q\mathcal{H}$ is a stationary point of this operator. Stated another way, $(\mathcal{H}'Q\mathcal{H})^2 = \mathcal{H}'Q\mathcal{H}$.

In more practical terms, an investigation of the vectors in the range of $\mathcal{H}'$ sgn is actually an investigation of the ensemble of possihle differential pictures which the proposed system might produce as output. This set is identical to the set of differential pictures which the system will encode and decode with zero error.

If $\mathfrak{H}$ is an $n \times n$ Hadamard matrix, then there are 2^n vectors in the range of $\mathfrak{H}^t$ sgn. For reasonable values of n, 2^n is so large that a complete listing of all of these vectors is not feasible. Fortunately, however, these 2^n vectors fall into a relatively small number of classes, each class consisting of those vectors which have the same *distribution* of magnitudes of component amplitudes. The problem of determining the possible distributions of magnitudes of the component amplitudes of a vector in the range of $\mathfrak{H}^t$ sgn turns out to be identical to the problem of determining the weight enumerators for the cosets of the Reed-Muller code. This equivalence is seen as follows: If $\mathbf{y}$ is a real vector whose components have unit magnitude, then the number of components of $\mathfrak{H}^t\mathbf{y}$ with magnitude $| A |$ is the number of rows of $\mathfrak{H}$ whose dot product with $\mathbf{y}$ is $\pm A$. On the other hand, if we convert 1 to 0 and -1 to 1, changing $\mathfrak{H}$ to $\mathfrak{G}$ and $\mathbf{y}$ to $\mathbf{R}$, then the weight of the binary vector sum of $\mathbf{R}$ and each codeword of the extended max-length feedback shift register code gives the distance between the received word $\mathbf{R}$ and the corresponding codeword, and the enumeration of all of these weights for a particular $\mathbf{R}$ is the weight enumerator for the coset containing $\mathbf{R}$. If $\mathbf{c}$ is a binary codeword for which $w(\mathbf{c} + \mathbf{R}) = d$ and if $\mathbf{u}$ is the real vector of ± 1's corresponding to $\mathbf{c}$, then $\mathbf{u}$ and $\mathbf{y}$ disagree in d components and agree in $n - d$ components. Therefore,

$$\mathbf{u} \cdot \mathbf{y} = n - 2d.$$

Since the first order Reed-Muller code contains both the codewords in the extended maximum length feedback shift register code and their complements, there is a one to one correspondence between RM cosets with weight enumerator $d_0, d_1, \cdots, d_n$ and real vectors in the range of $\mathfrak{H}^t$ sgn having magnitudes of component amplitudes distributed as follows: d_i components with amplitudes $\pm(n - 2i)$ for $i = 0, 1, 2, \cdots, n/2 - 1$, and $d_{n/2}/2$ components with amplitude zero.

The coset weight enumerators for first order RM codes of lengths up to 16 have been determined by R. Dick and N. J. A. Sloane.[11] Their results, and the corresponding distributions of magnitudes of amplitude components of the output of the differential picture encoding-decoding system are shown in Table I. Those rows which are predicted by our main theorem have been checked, and the relevant values of m have been listed.

The coset weight enumerator for the first order RM code of length 32 was determined by Berlekamp and Welch,[12] and the results are shown in Table II.

The coset weight enumerators for first order RM codes of length

TABLE I—COSET WEIGHT ENUMERATORS FOR FIRST ORDER RM CODES OF LENGTHS 4, 8 AND 16

Number of vectors in range of $\mathfrak{X}^t$ Sgn	Number of cosets										Value of m if predicted by main theorem
		$n = 4$									
		Amplitude	± 4		± 2		0				
		Weight	0 & 4		1 & 3		2 (entries halved)				
8	1		1				3				0
8	1				4						1
		$n = 8$									
		Amplitude	± 8		± 6		± 4		± 2	0	
		Weigbt	0 & 8		1 & 7		2 & 6		3 & 5	4 (entries halved)	
16.1	1		1							7	0
16.8	8				1				7		—
16.7	7						4			4	1
		$n = 16$									
		Amplitude	± 16	± 14	± 12	± 10	± 8	± 6	± 4	± 2	0
		Weight	0 & 16	1 & 15	2 & 14	3 & 13	4 & 12	5 & 11	6 & 10	7 & 9	8 (entries halved)
32.1	1		1								15
32.16	16		1							15	
32.120	120				1				7		8
32.560	560					1		3		12	
32.840	840						2		8		6
32.35	35						4				12
32.448	448							6		10	
32.28	28								16		

Value of m if predicted by main theorem
0
1
0
—
1
0
1
2

$\geqq 64$ have not yet been determined. This problem definitely merits further research.

VI. ACKNOWLEDGMENTS

I am indebted to Mr. J. R. Pierce for suggesting this problem and to Mr. N. J. A. Sloane for suggestions which simplified the proof of the identity in Appendix A.

APPENDIX A

A Sketched Proof of Main Result

One of the implications of our main theorem is that if β lies outside of the affine subspace spanned by the relevant α's, then $z_\beta = 0$. A generalization of this result is the following:

Theorem: If the only nonzero components of v all lie in a $(k-1)$ dimensional affine subspace and β lies outside of this subspace, then $z_\beta = 0$.

Proof: Using the elementary properties of RM codes and affine subspaces, the original $2^k \times 2^k$ Hadamard matrix may be partitioned as

$$\mathcal{H} = \begin{bmatrix} \mathcal{G} & \mathcal{G} \\ \mathcal{G} & -\mathcal{G} \end{bmatrix}$$

where $\mathcal{G}$ is a $2^{k-1} \times 2^{k-1}$ Hadamard matrix. In terms of this partition, the last 2^{k-1} components of $\mathbf{v}$ are zero and $\mathcal{H}\mathbf{v}$ is of the form $[\mathbf{w}, \mathbf{w}]^t$ for some appropriate 2^{k-1}-dimensional vector $\mathbf{w}$. We then obtain

$$\mathcal{H}^t \operatorname{sgn} [\mathbf{w}, \mathbf{w}]^t = 2[\mathbf{z}, 0]^t$$

where

$$\mathbf{z}^t = \mathcal{G}^t \operatorname{sgn} \mathbf{w}^t.$$

By repeated application of this theorem, we deduce that $z_\beta = 0$ unless β is in the affine subspace spanned by the coordinates of the nonzero components of $\mathbf{v}$. If the coordinates of the nonzero components of $\mathbf{v}$ span a d-dimensional affine subspace, then an appropriate change of coordinates allows us to work with a $2^d \times 2^d$ Hadamard submatrix, which is also Hadamard. The original output $\mathbf{z}$ vector merely gains a factor of two for each omitted dimension.

Applying these arguments to the main theorem of the text allows us to confine our attention to the case when $k = 2m$.

Since the RM code is invariant under the full affine group, there is

TABLE II—COSET WEIGHT ENUMERATORS FOR FIRST ORDER RM CODES OF LENGTH 32

Boolean function for coset*	Number of such cosets	Weights									Value of m if predicted
Even Cosets		0 32	2 30	4 28	6 26	8 24	10 22	12 20	14 18	16 (halved)	
2345	496 × 1	0	1	0	0	0	0	0	15	16	
2345&12	496 × 120	0	0	0	0	2	2	0	14	14	
2345&23	496 × 35	0	0	0	1	0	3	0	12	16	
2345&23&45	496 × 28	0	0	0	0	0	6	0	10	16	2
2345&12&34	496 × 840	0	0	0	0	0	2	8	14	8	
2345&123	17360 × 2	0	0	1	0	0	0	3	16	12	
2345&123&12	17360 × 24	0	0	0	1	0	1	4	14	12	
2345&123&24	17360 × 18	0	0	0	0	2	0	4	16	10	
2345&123&14	17360 × 192	0	0	0	0	1	2	4	14	11	
2345&123&45	17360 × 32	0	0	0	0	0	4	4	12	12	
2345&123&12&34	17360 × 72	0	0	0	0	0	4	4	12	12	
2345&123&14&35	17360 × 576	0	0	0	0	0	2	8	14	8	
2345&123&12&45	17360 × 96	0	0	0	0	1	0	8	16	7	
2345&123&24&35	17360 × 12	0	0	0	0	0	0	12	16	4	
2345&123&145	13888 × 320	0	0	0	0	1	1	6	15	9	
2345&123&145&45	13888 × 32	0	0	0	1	0	0	6	15	10	
2345&123&145&24&45	13888 × 480	0	0	0	0	0	3	6	13	10	
2345&123&145&35&24	13888 × 192	0	0	0	0	0	1	10	15	6	
123	155 × 8	0	0	1	0	0	0	7	0	24	
123&45	155 × 512	0	0	0	0	0	4	0	28	0	
123&14	155 × 168	0	0	0	0	2	0	8	0	22	
123&14&25	155 × 336	0	0	0	0	0	0	16	0	16	
123&145	868 × 32	0	0	0	1	0	1	0	30	0	
123&145&23	868 × 320	0	0	0	0	1	0	12	0	19	
123&145&24	868 × 480	0	0	0	0	0	4	0	28	0	
123&145&23&24&35	868 × 192	0	0	0	0	0	0	16	0	16	
12	1 × 155	0	0	0	0	4	0	0	0	28	1
12&34	1 × 868	0	0	0	0	0	0	16	0	16	
—	1 × 1	1	0	0	0	0	0	0	0	31	0

* These functions are written in an abbreviated notation. For example, the second line, 2345&12 indicates that this equivalence class of cosets includes one coset whose members are the 64 Boolean functions of the form $X_2X_3X_4X_5 + X_1X_2 + AX_1 + BX_2 + CX_3 + DX_4 + EX_5 + F$, where A, B, C, D, E, and F are arbitrary binary elements.

no loss of generality in assuming that $\alpha_0 = 0$, that $\alpha_1, \alpha_2, \cdots, \alpha_{2m}$ are unit vectors, and that

$$v_{\alpha_l} = +1 \quad \text{for} \quad l = 0, 1, \cdots, 2m.$$

Any other case can be reduced to this case by an appropriate affine transformation of coordinates.

We now determine the distribution of the vector

$$\mathbf{x} = \mathcal{C}\mathbf{v}.$$

TABLE II—Cont'd

Odd Cosets†		1 31	3 29	5 27	7 25	9 23	11 21	13 19	15 17	
—	32 × 1	1	0	0	0	0	0	0	31	
12	32 × 155	0	0	0	1	3	0	0	28	
12&34	32 × 868	0	0	0	0	0	6	10	16	
123	4960 × 1	0	1	0	0	0	0	7	24	
123&12	4960 × 7	0	0	1	0	0	3	4	24	
123&14	4960 × 84	0	0	0	1	1	2	6	22	
123&45	4960 × 64	0	0	0	0	3	1	7	21	
123&14&25	4960 × 336	0	0	0	0	0	6	10	16	
123&12&45	4960 × 448	0	0	0	0	1	3	13	15	
123&12&34	4960 × 84	0	0	0	0	2	4	4	22	
123&145	27776 × 10	0	0	0	1	1	0	12	18	
123&145&12	27776 × 6	0	0	1	0	0	1	10	20	
123&145&23	27776 × 80	0	0	0	1	0	3	9	19	
123&145&45&23	27776 × 16	0	0	0	1	0	1	15	15	
123&145&24	27776 × 180	0	0	0	0	2	2	10	18	
123&145&24&23	27776 × 240	0	0	0	0	1	5	7	19	
123&145&35&24	27776 × 240	0	0	0	0	1	3	13	15	
123&145&35&24&23	27776 × 192	0	0	0	0	0	6	10	16	
123&145&45&35&24&23	27776 × 60	0	0	0	0	0	4	16	12	

† All functions representing odd cosets also contain the term 12345, which is not shown in this table.

Since $\mathbf{x}$ is the sum of the all-ones vector (corresponding to the column of $\mathfrak{C}$ associated with $\alpha_0 = 0$) and $2m$ columns of $\mathfrak{C}$ which correspond to linearly independent codewords in the RM code, it is readily seen that there are $\binom{2m}{t}$ components of $\mathbf{x}$ which have the value $2m + 1 - 2t$. It follows that $\mathbf{y} = \operatorname{sgn} \mathbf{x}$ has $\sum_{t=0}^{m} \binom{2m}{t}$ $+1$'s and $\sum_{t=m+1}^{2m} \binom{2m}{t}$ -1's.

For convenience, we may partition the components of $\mathbf{y}$ into $2m + 1$ subsets, each of which corresponds to the components of $\mathbf{x}$ with the same value. We call the set which consists of $\binom{2m}{m}$ components where $\mathbf{x}$ had value $+1$ the "significant" set of components. The sets of insignificant components may be matched up in pairs; the set where $\mathbf{x}$ had value $2m + 1 - 2t$ being matched with the set where $\mathbf{x}$ had value $2m + 1 + 2t$. Each of these matched sets contains $\binom{2m}{t}$ components.

We now let β be a typical $2m$-dimensional binary vector, which is the sum of $2j+1$ α's. By an appropriate permutation of basis vectors, we may assume that

$$\beta = \alpha_0 + \sum_{i=1}^{2j} \alpha_i = \sum_{i=1}^{2j} \alpha_i .$$

The equation $\mathbf{z} = \mathfrak{C}^t \mathbf{y}$ now allows us to compute z_β as the dot product of a particular row of $\mathfrak{C}^t$ and $\mathbf{y}$. The equation $\beta = \sum_{i=1}^{2j} \alpha_i$ and the correspondence to RM codes allows us to express the particular row

of $\mathcal{H}^t$ under consideration as the componentwise product of the first $2j$ rows of $\mathcal{H}^t$, ignoring the zeroth row, which is all plus one. Symbolically, if we let $\mathbf{r}_1, \mathbf{r}_2, \cdots, \mathbf{r}_{2m}$ denote the first $2m$ rows of $\mathcal{H}^t$, then

$$z_\beta = (\mathbf{r}_1 \otimes \mathbf{r}_2 \otimes \cdots \otimes \mathbf{r}_{2j}) \cdot \operatorname{sgn} \left(\sum_{i=1}^{2m} \mathbf{r}_i \right)$$

where "$\otimes$" denotes the componentwise product. Since $2j$ is even, we may also write

$$z_\beta = [(-\mathbf{r}_1) \otimes (-\mathbf{r}_2) \otimes \cdots \otimes (-\mathbf{r}_{2j})] \cdot \operatorname{sgn} \left(\sum_{i=1}^{2m} \mathbf{r}_i \right).$$

The dot product is the sum over all 2^{2m} components of the componentwise product of $(\mathbf{r}_1 \otimes \mathbf{r}_2 \otimes \cdots \otimes \mathbf{r}_{2j})$ and $\mathbf{y} = \operatorname{sgn} (\sum_{i=1}^{2m} \mathbf{r}_i)$. Since there is cancellation of the summands coming from matched sets of components into which we partitioned $\mathbf{y}$, we need only consider the $\binom{2m}{m}$ "significant" components. On each of these, $\mathbf{y}$ takes value $+1$, and the problem reduces to the following: Given a $2m \times \binom{2m}{m}$ matrix, whose columns represent all ways of distributing m plus ones and m minus ones among $2m$ rows, compute the sum of the entries in the componentwise product of the first $2j$ rows of this matrix. The solution is obtained by noting that if there are i minus ones in the first $2j$ rows, then the componentwise product is $(-1)^i$ and this happens in $\binom{2j}{i}\binom{2m-2j}{m-i}$ columns. Therefore,

$$z_\beta = \sum_i (-1)^i \binom{2j}{i} \binom{2m - 2j}{m - i}.$$

Having already explained the other factors in the more general version of the theorem stated in the text, the theorem is reduced to the identity,

$$\sum_i (-1)^i \binom{2j}{i} \binom{2m - 2j}{m - i} \stackrel{?}{=} \frac{(-1)^j (2m - 2j)!\,(2j)!}{j!\,m!\,(m - j)!}.$$

Multiplying through by $(m!)^2/(2m - 2j)!(2j)!$ reduces this to the equivalent identity,

$$\sum_i (-1)^i \binom{m}{i} \binom{m}{2j - i} \stackrel{?}{=} (-1)^j \binom{m}{j},$$

whose proof is given by Riordan (p. 14, line 7 from bottom).[13] Q.E.D.

APPENDIX B

An Example

Suppose that the differential picture consists of a 4×4 grid, the points of which are lettered as follows:

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

The signs of the units in the 16 × 16 cyclic Hadamard matrix with which the differential picture is smeared may be taken as:

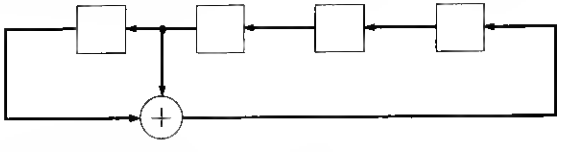
$\mathfrak{H} =$

+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
+	+	+	+	−	+	+	−	−	+	−	+	−	−	−	−
+	+	+	−	+	+	−	−	+	−	+	−	−	−	−	+
+	+	−	+	+	−	−	+	−	+	−	−	−	−	+	+
+	−	+	+	−	−	+	−	+	−	−	−	−	+	+	+
+	+	+	−	−	+	−	+	−	−	−	−	+	+	+	−
+	+	−	−	+	−	+	−	−	−	−	+	+	+	−	+
+	−	−	+	−	+	−	−	−	−	+	+	+	−	+	+
+	−	+	−	+	−	−	−	−	+	+	+	−	+	+	−
+	+	−	+	−	−	−	−	+	+	+	−	+	+	−	−
+	−	+	−	−	−	−	+	+	+	−	+	+	−	−	+
+	+	−	−	−	−	+	+	+	−	+	+	−	−	+	−
+	−	−	−	−	+	+	+	−	+	+	−	−	+	−	+
+	−	−	−	+	+	+	−	+	+	−	−	+	−	+	−
+	−	−	+	+	+	−	+	+	−	−	+	−	+	−	−
+	−	+	+	+	−	+	+	−	−	+	−	+	−	−	−

The induced coordinatization may be read from the 2nd, 3rd, 4th and 5th rows. It is:

Grid Point	Coordinatization	Representation as Sum of Odd Number of Affine Basis Vectors
A	0 0 0 0	H + I + L
B	0 0 0 1	E + H + I + L + P
C	0 0 1 0	H + L + P
D	0 1 0 0	E + I + L
E	1 0 0 1	E
F	0 0 1 1	E + H + L
G	0 1 1 0	E + L + P
H	1 1 0 1	H
I	1 0 1 0	I
J	0 1 0 1	I + L + P
K	1 0 1 1	E + I + P
L	0 1 1 1	L
M	1 1 1 1	H + I + P
N	1 1 1 0	E + H + I
O	1 1 0 0	E + H + P
P	1 0 0 0	P

The coordinates of B through P may also be taken as the successive contents of this shift register:



Now suppose the differential picture is this:

0	0	0	0
+1	0	0	−1
+1	0	0	−1
0	0	0	−1

The coordinates of the nonzero inputs are as follows:

E 1 0 0 1

H 1 1 0 1

I 1 0 1 0

L 0 1 1 1

P 1 0 0 0

0 0 0 1 = sum

These are affine independent, so our main theorem applies. The stray output pulse will be located at point B, since this is the point whose coordinates are the vector sum of the coordinates of the other inputs.

We now calculate the output vector step by step, witbout using the theorem. The input picture is:

$$\mathbf{v} = [0, 0, 0, 0, +1, 0, 0, -1, +1, 0, 0, -1, 0, 0, 0, -1].$$

The "smeared picture" is $\mathbf{x} = \mathfrak{C}\mathbf{v}$, which is given by the sum of the following rows:

$$\begin{array}{cccccccccccccccc}
+ & - & + & + & - & - & + & - & + & - & - & - & - & + & + & + \\
- & + & + & - & + & - & + & + & + & + & - & - & - & + & - & - \\
+ & - & + & - & + & - & - & - & - & + & + & + & - & + & + & - \\
- & - & + & + & + & + & - & - & - & + & - & - & + & + & - & + \\
- & + & - & - & - & + & - & - & + & + & - & + & - & + & + & +
\end{array}$$

$$\mathbf{x} = -1,-1,+3,-1,+1,-1,-1,-3,+1,+3,-3,-1,-3,+5,+1,+1$$

The quantized smeared picture is

$$\mathbf{y} = Q\mathbf{x}$$

$$= [- \; - \; + \; - \; + \; - \; - \; - \; + \; + \; - \; - \; - \; + \; + \; +].$$

The decoded differential picture is given by

$$\mathbf{z} = \mathfrak{C}\mathbf{y}$$

$$= [-2, -6, +2, +2, +6, -2, -2, -6, +6, -2, +2, -6, -2, +2, -2, -6].$$

When scaled down by a factor of six and placed on the grid, the output is

$-\frac{1}{3}$	-1	$+\frac{1}{3}$	$+\frac{1}{3}$
$+1$	$-\frac{1}{3}$	$-\frac{1}{3}$	-1
$+1$	$-\frac{1}{3}$	$+\frac{1}{3}$	-1
$-\frac{1}{3}$	$+\frac{1}{3}$	$-\frac{1}{3}$	-1

In order to match the total power of the input, the output must he scaled down slightly more.

REFERENCES

1. Schroeder, M. R., unpublished work.
2. Pratt, W. K., Kane, J., and Andrews, H. C., "Hadamard Transform Image Coding," Proc. IEEE, *57*, No. 1 (January 1969), pp. 58–68.
3. Hall, M., Jr., *Combinatorial Theory*, Waltham, Massachusetts: Blaisdell Publishing Co., 1967.
4. Spence, E., "A New Class of Hadamard Matrices," Glasgow Matb. J., *8*, Part I (January 1967), pp. 59–62.
5. Goethals and Seidel, J. J., "Orthogonal Matrices With Zero Diagonal," Canadian J. Math., *19*, No. 5 (1967), pp. 1001–1010.
6. Wallis, J., "A Class of Hadamard Matrices," J. Combinatorial Tbeory, *6*, No. 1 (January 1969), pp. 40–44.
7. Wallis, J., "Note of a Class of Hadamard Matrices," J. Combinatorial Theory, *6*, No. 2, (March 1969), pp. 222–223.
8. Thoene, R., and Golomb, S. W., "Search for Cyclic Hadamard Matrices," JPL Space Programs Summary, *4*, No. 37–40 (1966), pp. 207–208.
9. Baumert, L. D., "Cyclic Hadamard Matrices," JPL Space Programs Summary, *4*, No. 37-40 (1966), pp. 311–314.
10. Berlekamp, E. R., *Algebraic Coding Theory*, New York: McGraw-Hill, 1968.
11. Dick, R., and Sloane, N. J. A., unpublished work.
12. Berlekamp, E. R., and Welch, L. R., unpublished work.
13. Riordan, J., *Combinatorial Identities*, New York: Wiley, 1968.